How Do Undergraduate Students Construct Their View of Cybercrime? Exploring Definitions of Cybercrime, Perceptions of Online Risk and Victimization

Georgia Conway and Dr. Lee Hadlington

Abstract While cybercrime is recognized as an increasing problem in society, it is unclear how users perceive cybercrime and online risks. This qualitative study explored how undergraduate students in England, a group who are at relatively high risk of victimization, viewed language and concepts associated with cybercrime. Three focus groups were conducted with a total of 16 18- to 21-year-old undergraduate students, and data were analyzed inductively and thematically. The themes explored in this article include: the physical world versus the virtual world; confusion regarding the law (including a perceived lack of police interest in responding to cybercrime); the normalization of risky or harmful online behaviour; and victimization. The themes also point towards a variety of misconceptions about cybercrime alongside an ambivalence towards the potential risk of becoming a victim. The data provide a potential step towards tailoring education packages and awareness programmes to ensure at-risk groups are equipped with actionable mechanisms to protect themselves. Further research is suggested in terms of exploring how such perceptions can be changed through effective training and awareness programmes, potentially reducing the level of risk in this group.

Introduction

Over the past decade, the increasing threats to national infrastructure from potential cyber-attacks have positioned the issue at the highest tier of concern for the UK government (National Cyber Security Strategy, 2016). A critical issue is how to convey information about such threats to a wider audience, a point hindered by the lack of agreement in the terminology being used (Wall, 2008a, b). In the Cyber Crime Strategy (Home Office, 2010), it was suggested that crime should not be defined by the medium through which it is conducted, but should aim to ‘raise public confidence in the safety and security of the internet’ (p. 17). Despite this, a tendency to look at cybercrime through a traditional lens persists, not only hindering aspects of investigation and prosecution, but also effective communication (Gottschalk, 2010).

Despite official guidance, the general public’s behaviour regarding cybersecurity still falls short of the ‘best practice’ presented in numerous government led cybersecurity campaigns (Furnell and...
Moore, 2014). This may be due to strategies focusing on narrow, technological definitions of cybercrime that largely ignore aspects of human factors (Mittu and Lawless, 2015). Human factors are the most exploited in cybercrime and seen as the weakest link in cybersecurity (Oltramari et al., 2015; Happ et al., 2016). For example, research by Happ et al. (2016) found that when given a small incentive, people were willing to divulge their passwords to strangers. Therefore, it could be argued that weaknesses in cybersecurity are a result of limited relevant information rather than lack of good practice.

One of the key barriers to providing individuals with targeted information is a lack of understanding of how individuals view their risk from cybercrime (Wall, 2008a). By gaining a clearer and more detailed insight into how individuals define and understand cybercrime, mechanisms for the development of more targeted and developed communication packages can be designed (Hadlington and Chivers, 2018). However, studies exploring the experiences and perceptions of at-risk populations are severely limited, making the development of such packages difficult. It is from this perspective that the current research is presented, with a key focus on one specific at-risk group, that of undergraduate students (Bidgoli et al., 2016; Hadlington and Chivers, 2018).

Definitions and classifications of cybercrime

The topic of cybercrime has become a critical focus for many, including researchers, law enforcement, and those developing government policies. Despite this, cybercrime lacks a universally accepted definition (Gordon and Ford, 2006; McQuade, 2007). This lack of agreement regarding the definition of cybercrime has been linked to public confusion in relation to which behaviours or actions fall under the category (Wall, 2008a, b). The term is often used to describe crimes involving computers (McQuade, 2007), but can be used to refer to a much broader set of crimes. Cybercrime does not only refer to the use of the Internet to commit crime, but also can be viewed as existing on a continuum (Gordon and Ford, 2006). This can range from aspects of ‘technological crime’ (also referred to as cyber-dependent crime; NCA, 2016) that can only exist within a system such as the Internet, or hardware and software. At the other end of the spectrum, there is ‘people crime’ (or cyber-enabled crime; NCA, 2016) in which technology or the use of the Internet is only a minor part of the crime. It is clear that there are a number of overlapping and competing terms prevalent in the literature, which in turn proliferate confusion for users, which in turn may influence the way in which cybercrime is perceived.

Public perceptions of cybercrime

News articles on the topic of cybercrime are often given top priority due to the pervasiveness of digital technology in modern life. However, commentators have noted that this may serve to reflect an unrealistic level of cybercrime victimization (Wall, 2008a). The over-exuberant reporting of cybercrime by the mass media may lead to an assumption that cybercrime is extremely prevalent, in turn creating undue fear among the public (Wall, 2008b; Yu, 2014). In this context, cybercrime is viewed as an emotive construct, where the primary emotion being evoked is that of fear (Burrows, 1997; Wall, 2007). In contrast, academic literature and government policy focus on the scientific definitions, explanations, and strategies involving cybercrime (Wall, 2007). This discrepancy may impact on the successful communication of information from academic and legislative resources to the public, in turn explaining why there is a heavy reliance on other sources such as the mass media (Wall, 2008a; Hasan et al., 2015).

Previous research has noted that information on cybercrime comes from misleading sources, for example, popular television and film (Penfold-Mounce et al., 2011). Wall (2008b) noted a heavy reliance on aspects he terms as ‘social science fiction’, a branch of science fiction that explores
societal issues against a backdrop of technical change and technical possibilities. This aspect then becomes intertwined with both cybercrime and technology growth, permeating an image of cybercrime that is both unrealistic and apprehensive (Burrows, 1997; Wall, 2008b). Fiction has also created stereotypical descriptions of cybercrime and the perpetrators. Cybercriminals are stereotypically described as hackers and loners who are immersed in cyberspace and living in a dystopic future (Wall, 2008b). From this perspective, the public perception of cybercrime is often masked in hype and unrealistic portrayals, making the issue of communicating prevention packages difficult.

**Undergraduate students’ risk of victimization from cybercrime**

Those who use digital technology frequently are most at risk of being a victim of cybercrime, and are in turn less likely to be aware of the risks associated with digital technology and the Internet (Hargittai and Hinnant, 2008; Friemel, 2016; Riek et al., 2016). One particular group that has a heightened risk of susceptibility to cybercrime is undergraduate students. Research by Bidgoli et al. (2016) noted that undergraduate students in particular are more vulnerable to cybercrimes due to a heightened engagement with technology, newfound financial, and social independence. Bidgoli et al. (2016) noted that over half of their sample had experienced at least one form of cybercrime while studying. It was also noted that this group rely heavily on the media and people they know personally for their information about cybercrime and cybersecurity. Bidgoli et al. (2016) also found that the majority of students lacked the relevant knowledge on how to officially report a cybercrime.

This perspective is placed in stark contrast to the stereotypical view that it is those in the age bracket of >60 years who are more likely to be the victims of cybercrime. Fraudscape, CIFAS, 2017 (Cifas, 2017; Experian, 2017). Data from the credit agency Experian (2017) (https://www.experianplc.com/media/news/2017/fraudsters-target-twenty--somethings/) showed that those in the 20–29 age bracket had experienced a 5.7% rise in fraudulent attacks since 2014. Shared accommodation, a lack of monitoring financial statements, and living their lives online all served to increase young people’s susceptibility to online crimes. In the annual Fraudscape report produced by Cifas (2017) it was also highlighted that individuals in there 30s were at greater risk of identity theft, again challenging the notion that it is the elderly who are more vulnerable to such attacks. Therefore, this article contributes to literature on cybercrime victimization by offering a contextual understanding of undergraduate students’ perceptions of cybercrime via qualitative research involving focus groups with students in England.

**Aims and objectives**

The current study aims to explore how a group of undergraduate students perceived and construct their view of cybercrime and cybersecurity. Researchers have noted that more effort needs to be focused on educating young adults as to the potential risks presented by cybercrime (McQuade, 2007). By doing so, an enhanced level of digital security can be established through tailored educational programmes, providing a potential mechanism for decreasing the risk of victimization (Wiederhold, 2014). In order to achieve this, there is a need to gain a clearer understanding of how young adults formulate their definitions of cybercrime as well as their understanding of key terms aligned to this. It is also important to assess how they perceive risk online, with previous research also noting that this age group is particularly prone to engaging in activities that could leave them open to victimization (McQuade, 2007). In this qualitative study, the following research questions were explored: ‘what does the term cyber mean to young people?’; ‘how do young people perceive cybercrime?’; and ‘who do you think is most at risk to threats online?’
Methods

Three focus groups were conducted with undergraduate students from one university in England. Sixteen participants (7 males and 9 females) aged between 18 and 21 years of age took part in the focus groups. Students were offered an incentive to participate in the study via the award of course credits for their participation where appropriate. Focus groups consisted of three mixed-sex focus groups of between four and seven participants.

Focus group questions were developed through a review of the literature in addition to consultations with specialist police officers in the area of cybercrime. They covered topics such as how individuals defined the concept of ‘cyber’ and cybercrime, who they thought was most at risk from cybercrime, and how they get their information about cybercrime. Each focus group lasted between 40 min in duration and was recorded on a dictaphone and a digital camcorder. The recordings were then transcribed verbatim.

Data were analysed using inductive thematic analysis, following the steps outlined by Braun and Clarke (2006) which include: familiarization with the data; generation of initial codes; searching for and creating themes; reviewing themes; and refining and naming the themes. Inductive thematic analysis is data driven; hence, an existing coding framework or the researcher’s preconceptions did not restrict the development of themes.

Pseudonyms have been utilized in order to protect the anonymity of the participants. Following university ethical approval, detailed information sheets were provided to participants outlining their right to withdraw and informed consent. After the focus group, participants were provided with a debrief sheet and invited to ask any questions they had before leaving.

Results

The analysis of the transcripts revealed a number of key themes. The first one was the physical world versus the real world, and details various perceptions that participants viewed the crimes conducted online as being very distinct and different to those occurring offline. A related subtheme, lack of confidence in the police to tackle cybercrime, includes the perception that the police lack the relevant technical skills and are disinterested in cybercrime. The second main theme that is presented here is that of an awareness of online risks in which participants explore the key risks they perceive online. Aligned with this is the subtheme of perceived safety through app use, outlining a preconception on the behalf of some participants that interactions conducted through smartphone-based applications were safer and offered more protection. The final theme is that of victim blaming and the perceptions of victimization of cybercrime in which participants explore the notion that victims of cybercrime are in some way at fault. This latter theme also includes a discussion related to who the participants felt were most at risk of becoming victims of cybercrime.

The physical world versus the virtual world

A common theme throughout the focus groups was the view that cyberspace as being separate from the physical world. For example, one participant presents the view that the online environment is:

A virtual reality, like it’s not exactly physical but parts of it are and it branches out. (Jack, FG1)

Similarly, Mona makes reference to the fact that the term ‘cyber’ conjures up the notion of:

Cyber Men ((laugh)) yeah (.) and things that aren’t really like real technology that’s advanced beyond the years. (Mona, FG2)

This view that concepts associated with the terminology of cyber as ‘things that aren’t really like real’ was prominent throughout the focus groups. The reference to ‘Cyber Men’ also serves to reiterate the public’s reliance on social science fiction (Wall, 2008b) as a
source of information, particularly in understanding unfamiliar language such as the term ‘cyber’ (Penfold-Mounce et al., 2011). It demonstrates the belief that for many, the cyber-world represents a distinct and non-physical environment to that of the ‘real world’. The perception of the cyber-environment as not being real may in turn result in individuals treating the threat of risk from such as limited or less serious to the risks in the offline world.

Participants also drew on their knowledge of traditional crime to anchor their understandings of cybercrime. Mona outlines her belief that the online environment could be used as a potential training mechanism for criminals to practice before engaging in a physical crime:

*I think as well for like other types of crime like you can use it as like a practice simulator kind of thing, so if you’re going to break into a bank (.) I know people don’t really do that anymore ((laughing)) but like to do that you could like make a game where you’ve got to try and get into a bank.* (Mona, FG2)

Cyberspace is viewed as a ‘practice simulator’, but there is no real acknowledgement of the risk posed by cyber-dependent crimes. The participant appears to believe that in order to perpetrate a crime, the actual crime still has to be physically conducted and is only simulated in the online environment. The participant also notes that, ‘people don’t really do that anymore’, in reference to physically robbing a bank, suggesting that crimes of this nature have shifted totally online.

The distinction between the physical world and cyberspace is more telling in the context of how participants viewed the concept of their finances. Kelly presents a more focused view of money in cyberspace against the physical possession of such:

*I think as well for like other types of crime like you can use it as like a practice simulator kind of thing, so if you’re going to break into a bank (.) I know people don’t really do that anymore ((laughing)) but like to do that you could like make a game where you’ve got to try and get into a bank.* (Mona, FG2)

Kelly’s first remark is telling, where she states that paying for things online, particularly in relation to mobile applications, is not really viewed as money. This belief also links to the ease of excessive spending online, where Kelly states that: ‘*all I have to do is press okay and it’s not money you just don’t think of it as money*’

The key aspect that underpins this theme is the view that cyberspace is viewed as separate from the physical world. Participants anchor their understanding of cybercrime in their experience and knowledge of traditional crime, in turn leading to gaps in knowledge and confusion (Ngo and Paternoster, 2011). Scholars, government, and law enforcement often use the term ‘cyber’ as a descriptive concept, and it is taken for granted that the general public are fully aware of what such a term refers to. This theme highlights the potential for confusion, with many participants viewing the term in the context of social science fiction and virtual reality (Burrows, 1997; Wall, 2007, 2008a).

**Lack of confidence in the police to tackle cybercrime.** Participants also demonstrated a widely held belief that the police are ill-equipped to deal with the growing threat posed by cybercrime. For example, Xander explains:

*S sometimes policing organisations may not be the best people to look at it sometimes because we’re also catching up because its new. There’s things happening in the cyberworld and offences taking place or not we’re trying to catch up on it and we’re trying to say well is that an offence? How do we investigate that?* (Xander, FG1)

Xander claims that the police may not be the most effective organization to deal with cybercrime, in part due to the newness of such technologies. There is the associated belief that legislators are slow to react to developments in cybercrime, making the process of reporting such even more difficult. This is particularly a salient issue and
presents a critical area for further exploration. If the public believes that both the police and the legal system are ineffective when it comes to dealing with aspects of cybercrime, then confidence will be lost and under-reporting will continue.

The notion that cybercrime was not being taken as seriously as crimes which have a clear ‘offline’ element was evident in further extracts from participants:

I think as well especially if you’re reporting to the police, it’s very hot right now only report emergencies and you feel like ah is this is this a real emergency because it’s not face-to-face it’s not a physical crime do they class it as a real emergency? (Ellie, FG2)

Or they maybe feel like it’s not real enough for to like nobody’s come and sort of punched you in the face, it’s over the internet it’s not. (Jo, FG3)

Both of these participants express the belief that because cybercrime is ‘not real enough’, as it is not physical and does not represent an emergency, it is not taken as seriously as offline, traditional crimes.

### Awareness of online risks
Participants discussed a variety of situations in which they or people they knew had engaged in risky or harmful online behaviour. Although this behaviour potentially placed them at increased risk of becoming a victim of cybercrime, their behaviour was justified for a number of reasons. Xander discussed the notion that many young people become immersed in the online digital environment, therefore are often unaware of the risks associated with being online:

I think certainly even though it’s within a lot of young people’s lives I think interestingly a lot might not be as aware of the actual danger involved in these things (...) it’s so, so normal as part of their lives to have these things they may not see the risks associated with each platform that they’re online so they’re probably more likely to be at risk from those things. (Xander, FG1)

Greg also highlights what he believes to be the current risks from being online, particularly when young people are spending a lot of time watching video bloggers:

What they see on these vlogs isn’t always real life cos I think a lot of young people watch those and think ah yeah this is what we need to do have all these accounts and everything’s great and it’s all a big happy life and then they feel if they’re not part of that that’s what can make them vulnerable to a lot of other issues. (Greg, FG1)

Greg indicates that the views and lifestyles that younger children are being exposed to via online media can make them ‘vulnerable to a lot of other issues’.

Jo also points to the risks of having and sharing information online:

I think everything is a risk [Mike: everything is a risk] you give so much information about yourself online and Facebook you can like tag your location you can tag where you’ve been where you’re going who you’re going with. (Jo, FG3)

There is an element of acceptance here that risk is an accepted part of being online, and is the by-product of activities involving aspects such as social networking.

### A perception of safety through app use
A further subtheme emerged, relating to dating sites and applications such as Tinder and Grindr. Tinder and Grindr are both applications that show users in the nearby locations in order for users to be able to meet in person (Farnden et al., 2015). It is often the
case that the use of these applications appears to encourage risky behaviour by presenting an illusion of safety through the use of an app. Mona demonstrates this point:

\[ I \text{ think as well the apps kind of make you feel safer about it (.) I know I've met people off those kind of apps and just kind of like wandered into their house because well... yeah they were nice. (Mona FG2)} \]

Mona appears to negate the potential risks of meeting a complete stranger and visiting their home as the interaction is mediated through the use of an app. This behaviour is justified through the feeling of safety the mobile application creates: ‘I think as well the apps make you feel safer about it’.

However, other participants were aware of the potential risks of meeting individuals that they have only conversed with online. For example, Tilly recounts the experience of a friend:

\[ ‘My friend met somebody on tinder and like he was proper forward and we’ll book a hotel room and whatever I was like she was like completely up for it and I was like NO do not do not... she’s in that mindset she uses it all the time and all of her friends at uni do she didn’t think twice about...’. (Tilly, FG3) \]

Tilly’s friend is unaware of the potential risks such a meeting poses. The willingness to engage in the action of meeting a potential stranger in a hotel room appears to be governed by accepted social norms, with Tilly describing the impression that ‘all of her friends at uni’ do it, so it was perceived to be safe.

**Victim blaming and the perceptions of victimization for cybercrime**

A further element that came through was the prevalence of victim blaming in the context of cybercrime. For example, Greg stated:

\[ There’s also a lot of victim blaming (.) and self-blame sometimes they think you know they don’t want to report it because they think they might have done something wrong.... they think maybe I’ve done something wrong and they feel like if I report it they might blame me so there’s kind of reluctance-y to go and get that reported cause they don’t know where they stand with the law. (Greg, FG1) \]

Greg suggests that aspects of victim blaming and self-blaming are commonplace. Alongside this is the assertion that a lack of understanding of the law has a role to play in the under-reporting of cybercrimes, particularly in terms of ‘they don’t know where they stand with the law’.

A variety of perspectives were presented as to why individuals become victims in the first instance. For example, Jack states that the older generation, who have had limited exposure to digital technology, are more vulnerable to being victims of cybercrimes due to being less technically savvy:

\[ I think it does come down to awareness and (. ) teaching people especially the older generation that haven’t had it growing up with them and might not know about these kind of scams and stuff and what can happen and don’t quite realise that the whole cyberspace is quite open. (Jack, FG1) \]

Other participants used the term ‘vulnerable’ but failed to follow this up with a clear description of who they thought fell into this grouping. One participant mentioned that ‘the older people that get targeted by spam emails and stuff...’ (Jo, FG3).

Victim blaming also resurfaced, with many participants referring to potential deficiencies in the knowledge or general awareness of victims. These aspects are displayed in the following extracts. For example:
I think it just all comes down to the naiveté of it and the comfort and how big the cyberworld is. (Jack, FG1)
I think it’s more of a thing where they don’t think it’ll happen to them so they’re naïve as to the fact yeah it’s out there and other people can be victims but it won’t happen to me. (Greg, FG1)

“So that they get the gullible people in order to like continue the process” (Jo, FG3)
“Yeah and they find out who’s who’s sort of the weakest and then people do just fall in love with the concept they’re like ah someone’s always there to talk to me” (Kelly, FG3)

Concepts such as gullibility, weakness, and naiveté are all mentioned in the context of cybercrime victimization. For many of the participants, the potential to become a victim of cybercrime was the result of an individuals’ failure to exercise self-awareness about the potential risks of being online.

Discussion
This article explored a number of key aspects related to the perceptions and attitudes towards cybercrime in a group of undergraduate students in England via qualitative research consisting of focus groups. Themes that were explored included: the physical world versus the virtual world; confusion regarding the law (including a perceived lack of police interest in responding to cybercrime); the normalization of risky or harmful online behaviour and; their perceptions of victimization.

Defining and understanding cybercrime—‘cyber men’ and ‘virtual reality’
Many of the participants drew on aspects and ideas from science fiction to shape their understanding of the term ‘cyber’. References made to concepts such as ‘cyber men’ and ‘virtual reality’ illustrate that the participants placed a heavy reliance on science fiction in order to frame an understanding of concepts associated with the term ‘cyber’. This tendency has been noted in previous research, particularly when individuals come into contact with terms they find unfamiliar (Penfold-Mounce et al., 2011). Reliance on concepts that are rooted in fiction rather than reality demonstrates one of the key issues that policy makers and law enforcement have to overcome when addressing critical points about cyber safety.

Participants also viewed concepts associated with the word ‘cyber’ as being on a distinct and different level to physical constructs in the ‘offline world’. This relationship between ‘cyber’/things that aren’t really real’, and the ‘offline’ ‘physical world’ demonstrates an additional gap in the language that is being used by official sources and the public understanding of such concepts (Wall, 2008a, b). This is further exacerbated by confusion regarding the nature of cyberspace, and whether it can be viewed as a further extension of the physical environment or acts as one that is separate and distinct (Yar, 2005). If this confusion exists alongside the belief that the cyber domain lacks physicality, then there is a risk that aspects of cybercrime are viewed as less serious. This may result in individuals having a more relaxed attitude towards their online safety and security, thus increasing their potential susceptibility to cybercrime.

Many participants also used concepts taken from aspects of traditional crime to shape their understanding of cybercrime, a tendency that has been noted in previous research (Howarth, 2006). In this instance, many participants already have existing and well-established knowledge or perceptions of the aspects of traditional crime, and so they anchor their understanding of the newer concept of cybercrime within this framework (Moscovici, 1988). For many individuals, there is a failure to recognize that many cybercrimes can be carried out only through the use of the Internet and digital technology, with existing preconceptions often leading to the bias that for a ‘crime’ to occur there needs to be an aspect of physical interaction.
The police are ill equipped to deal with cybercrime

Many of the participants in this study expressed the view that the police were ill-equipped to deal with cybercrime. The most frequently presented reason for this was the belief that the police are in a constant state of ‘catch-up’ as newer and more sophisticated forms of cybercrime emerge. This resonates with research conducted by Hadlington (2018) who found that many employees held the opinion that police lack the capacity to deal with cybercrime effectively. Similarly, Wall (2007) points to the long history of members of law enforcement voicing their concern about a lack of facilities which would enable them to keep track of newer offences. Wall also noted that there are a number of institutional barriers to the adoption of newer practices and technology, in particular the deep conservatism that governs their operations. It is therefore no surprise that the public perception of the police as being unable to respond in an agile and effective way to new threats, such as cybercrime, is common place. One of the consequences for such beliefs is that many individuals fail to report such crimes believing that the police lack the capacity to deal with them (Wall, 2007).

Victimization and cybercrime

In focus groups, discussion of who is most likely to be a victim of cybercrime relayed commonly held stereotypes. The often presented notion of a digital divided between ‘digital natives’ (who have never known a world without the Internet) and ‘digital immigrants’ (who have adopted digital technology later on in life) is often widely viewed as a reason for such differences in susceptibility to cybercrimes (Prensky, 2007). However, such a perspective may serve to create an illusion of safety for the younger generation who believe that they have the required expertise in aspects of digital literacy, and are therefore less likely to be targeted by cybercriminals. It has conversely been shown that it is more frequent Internet users who are more likely to become victims of cybercrime (Riek et al., 2016). The recent data from both Experian (2017) and Cifas (2017) on online fraud and identify theft also point towards a rise in attacks perpetrated against younger adults, suggesting that more preventative work needs to be done. All of the participants in the present study belonged to this age group, but did not recognize that they are at high risk of online victimization. Instead, they chose to direct higher risk of victimization towards the very young and the elderly.

Participants also discussed the concept of victim blaming. The concept of victim blaming has been noted as a common aspect in all crimes, but it appears that there is a significantly more victim blaming in the case of cybercrimes (Cross, 2015). For some participants, fears related to being unfamiliar with specific laws governing their activities online led them to believe that they might be blamed for falling foul to cybercrime. Other participants assumed that victims of cybercrime were ill equipped to deal with the activities they were engaged in online, and were gullible, silly, weak, and naïve.

Conclusion

It is evident that communicating the potential risks to the public, including the younger generations at risk of online victimization, about the risks from online crime, is fraught with difficulties. There appears to be a mismatch between the advice and information that is being sent out by government and law enforcement and individual awareness of the seriousness of online crime. It is acknowledged that this is a small-scale study; however, the results provide an important insight into the contextual factors shaping young people’s views of cybercrime. Further research is warranted to expand on several of the key findings from the present study. One crucial aspect for larger empirical data collection would be exploring how undergraduate students can be educated and trained in effectively in aspects
of online risk. The follow on to this research would be to explore if, and how, such interventions serve to alter their accepted perceptions of cybercrime. As noted, this particular group is at high risk of online victimization (including online fraud and theft), but the participants overlooked this fact due to their assumption that as ‘digital natives’ they were sufficiently technologically savvy and aware of the risks of online engagement. The results demonstrate that these participants tend to embed their understandings of cyber-related concepts in popular science fiction. They also express notions of cybercrime being taken less seriously by the authorities in contrast to traditional aspects of crime which were viewed as occurring in the physical/offline world.

References


Exploring definitions of cybercrime, perceptions of online risk, and victimization


